Wireshark 101

Jeffrey L Carrell

Network Instructor

jeff.carrell@teachmeipv6.com

https://github.com/jeffcarrell/Wireshark-101

Wireshark 101

- OSI
- Well-known ports
- IP Headers
- Install WireShark
- Sniffing (Promiscuous Mode)
- TCP handshake

Wireshark 101

- Filtering
- UDP, TCP, and ICMP scanning
- Socket connectivity
- Encapsulation
- Man in the Middle attacks discussion

OSI Model

APPLICATION	Applications Layer: deals with applications protocols or services common to applications protocols
PRESENTATION	Presentation Layer: agree on the form that data will be in
SESSION	Session Layer: sets up and manages coordinated connections between two or more programs
TRANSPORT	Transport Layer: takes end-to-end responsibility for messages
NETWORK	Network Layer: decides what is the next stop the messages must take to reach its destination, this includes translating names to addresses, and building & maintaining routing tables
DATA LINK	Link Layer: takes responsibility for the message reaching the next link correctly
PHYSICAL	Physical Layer: defines how bits are represented and what types of cable and connectors are used

Well-known ports

Protocol	TCP/UDP	Port Number
File Transfer Protocol (FTP)	TCP	20/21
Secure Shell (SSH)	TCP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name System (DNS)	TCP/UDP	53
Dynamic Host Configuration Protocol (DHCP)	UDP	67/68
Trivial File Transfer Protocol (TFTP)	UDP	69
Hypertext Transfer Protocol (HTTP)	TCP	80
Post Office Protocol (POP) version 3	TCP	110
Network Time Protocol (NTP)	UDP	123
NetBIOS	TCP/UDP	137/138/139
Internet Message Access Protocol (IMAP)	TCP	143
Simple Network Management Protocol (SNMP)	TCP/UDP	161/162
Border Gateway Protocol (BGP)	TCP	179
Lightweight Directory Access Protocol (LDAP)	TCP/UDP	389
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	TCP	443
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)	TCP/UDP	636
FTP over TLS/SSL	TCP	989/990

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

IP(v4) header

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Example Internet Datagram Header

https://tools.ietf.org/html/rfc791

Wireshark

- Install Wireshark
- Wireshark basics
- Wireshark: color rules, display filters, columns, configuration profiles, packet annotation, and capture filters
- Wireshark labs!!!

Getting Wireshark

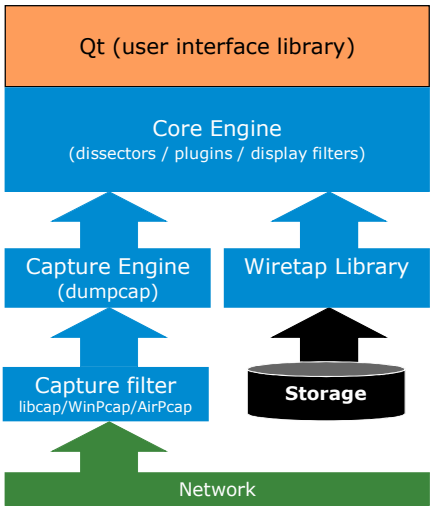
https://www.wireshark.org/download.html

Getting Wireshark

Vendor / Platform
Alpine / Alpine Linux
Apple / macOS
Arch Linux / Arch Linux
Canonical / Ubuntu
Debian / Debian GNU/Linux
The FreeBSD Project / FreeBSD
Gentoo Foundation / Gentoo Linux
HP / HP-UX
NetBSD Foundation / NetBSD
Novell / openSUSE, SUSE Linux
Offensive Security / Kali Linux
PCLinuxOS / PCLinuxOS
Red Hat / Fedora
Red Hat / Red Hat Enterprise Linux
Slackware Linux / Slackware
Oracle / Solaris 11

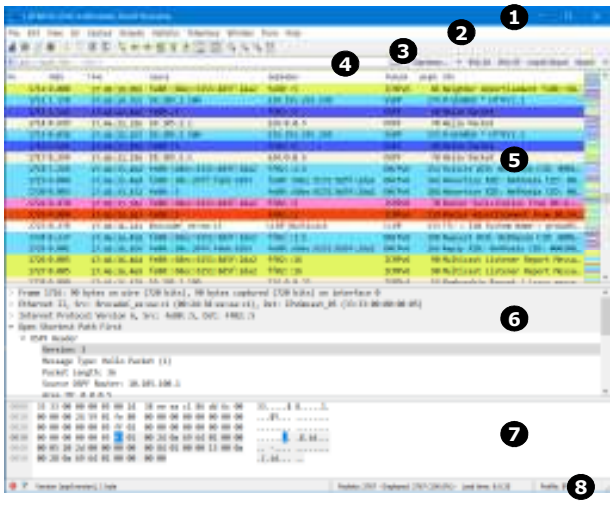
https://www.wireshark.org/download.html

Wireshark operations



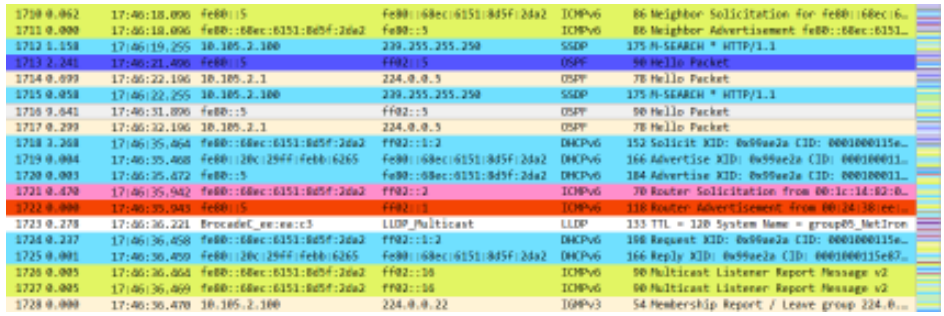
- When performing a live capture, you use one of three link layer drivers and go up through the Capture Engine (dumpcap).
- Dumpcap.exe is actually launched to do the capturing – wireshark.exe does not have capture capability.
- When you open a trace file from disk, capture filters cannot be used.
- Wireshark's Wiretap Library can recognize LOTS of trace file formats.
- Dissectors are the powerful elements that pick apart the contents of packets and display their field names and in some cases field interpretations.
- Display filters can be used whether you are performing a live capture or opening a saved trace file.

Wireshark main view



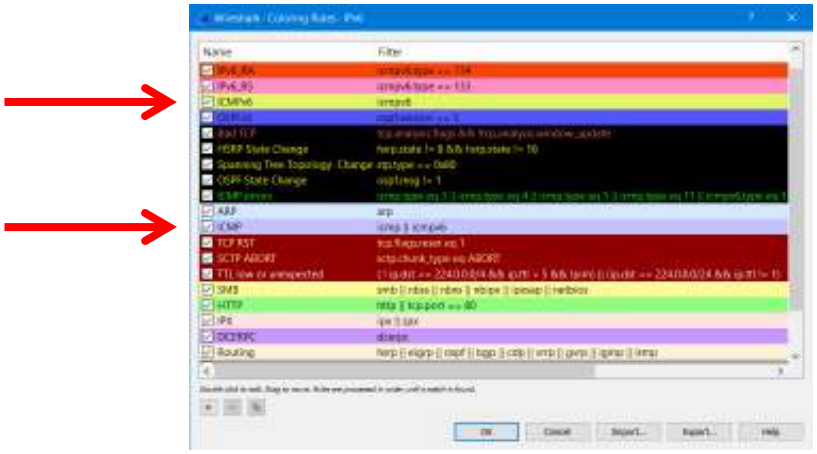
1. Title bar — trace file name or capture device name
2. Main menu — standard menu
3. Main toolbar — quick access
4. Display filter area — reduce the amount of traffic you see
5. Packet List pane — summary of each frame
6. Packet Details pane — dissected frames
7. Packet Bytes pane — hex and ASCII details
8. Status Bar — access to the Expert, annotations, file location, packet counts, and profiles

Coloring rules



- Colors help you focus on specific address, protocols, events, and possibly find errors quickly

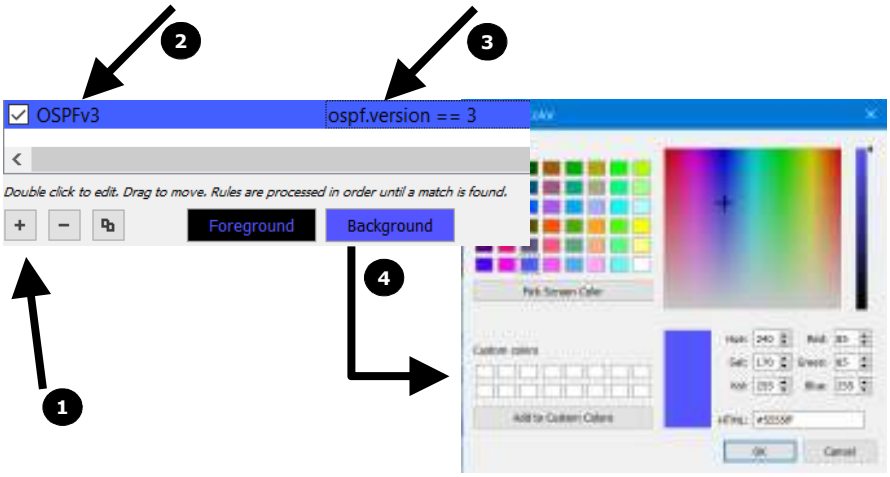
Color rule processing order



- Color rules read like a router ACL or firewall rules
  - First color rule that matches wins

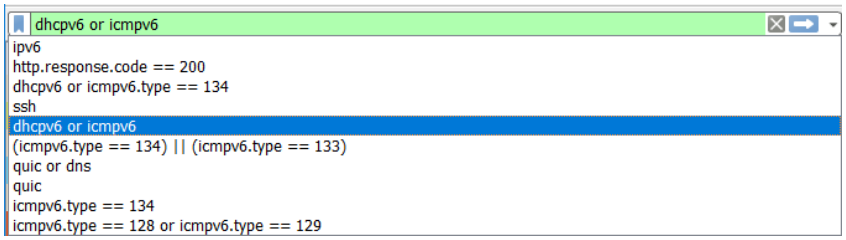
13

Color rule creation



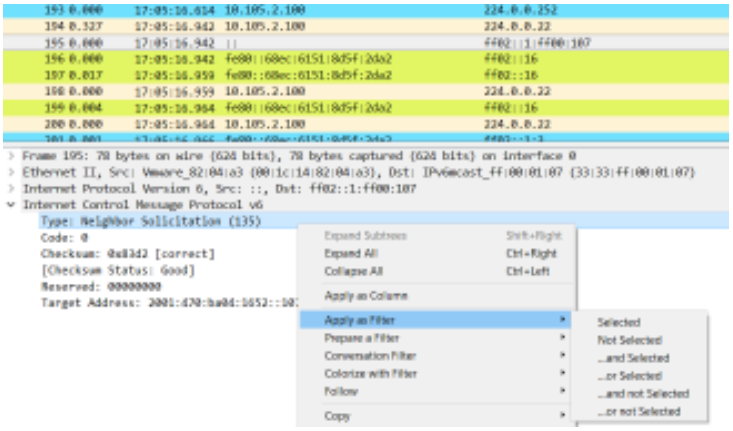
14

Display filters – option 1



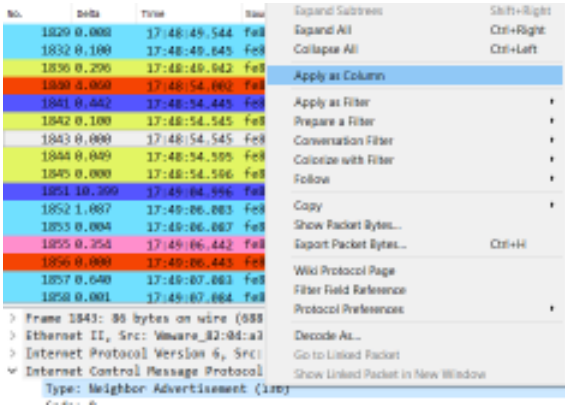
- The Filter bar will change colors as you type to signify correct syntax for the filter
  - Green – syntax is correct
  - Red – syntax is correct
  - Yellow – syntax is suspect
- The Filter dropdown will show last 10 filters used
- You can save Filter definitions for frequent use

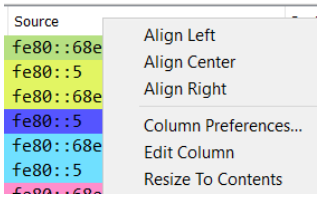
Display filters – option 2



- In the Packet Details view, right-click on a specific field to build a filter

Columns





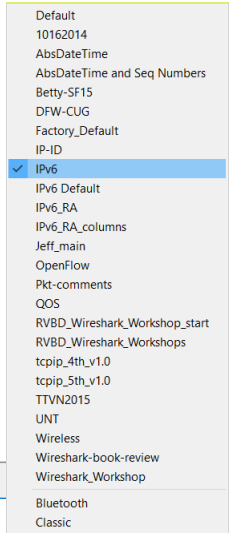
- Right-click column headings to sort, rename, align, etc

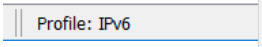
- In the Packet Details view, right-click on a specific field to Apply as Column

17

Configuration profiles

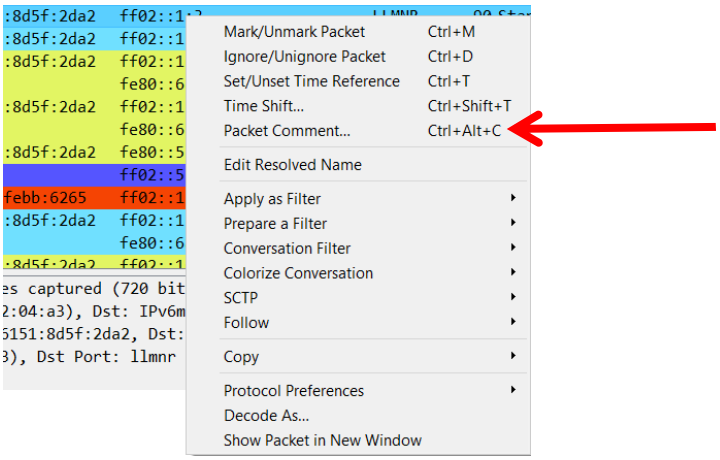
- What they are
- Why/how you use them
- What they contain
- How to share





18

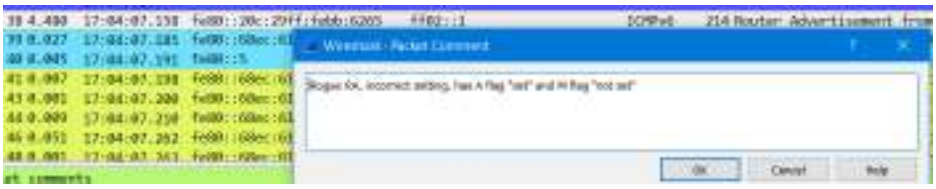
Packet annotation

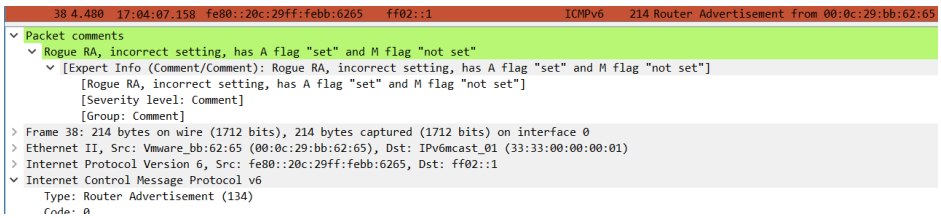


- Right click packet, select Packet Comment

 19

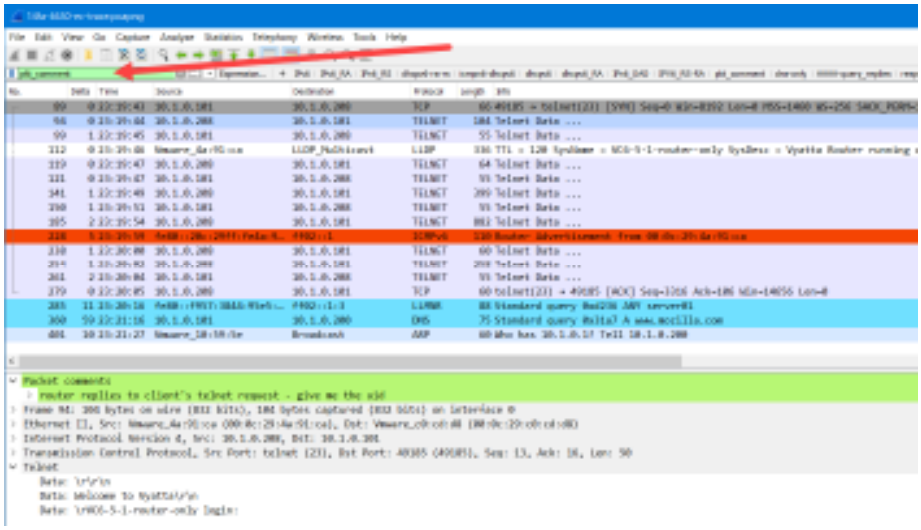
Packet annotation



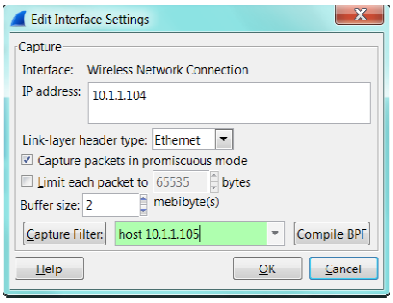


 20

Packet annotation display filter



Capture filters



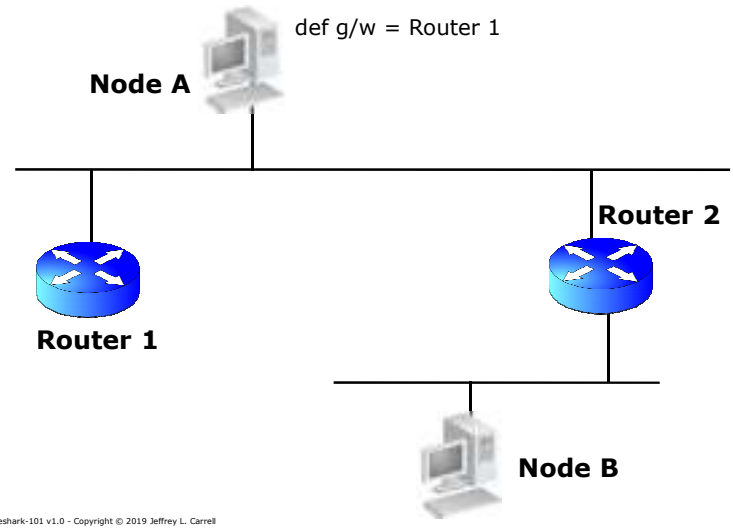
- To configure/apply a capture filter, double-click an adapter in the Capture Options window
- The Capture Filter bar will change colors as you type to signify correct syntax for the filter
  - Green – syntax is correct
  - Red – syntax is correct
  - Yellow – syntax is suspect
- To use a saved capture filter, click the Capture Filter button and select or type in info
- Use capture filters sparingly, as you could inadvertently miss traffic you needed to capture

Capture filters - examples

Capture Filter Example	Purpose
ether host 00:08:15:00:08:15	Capture traffic to or from hardware address 00:08:15:00:08:15
host 10.3.1.1	Capture traffic to/from 10.3.1.1
host 2406:da00:ff00::6b16:f02d	Capture traffic to/from the IPv6 address 2406:da00:ff00::6b16:f02d
not host 10.3.1.1	Capture all traffic except traffic to/from 10.3.1.1
src host 10.3.1.1	Capture traffic from 10.3.1.1
host 10.3.1.1 or host 10.3.1.2	Capture traffic to/from 10.3.1.1 and any host it is communicating with and traffic to/from 10.3.1.2 and any host it is communicating with
host www.espn.com	Capture traffic to/from any IP address that resolves to www.espn.com (this will only work if the host name can be resolved by Wireshark prior to capture)
net 10.3.0.0/16	Capture traffic to/from any host on network 10.3.0.0
port 53	Capture UDP/TCP traffic to or from port 53 (typically DNS traffic)
tcp port 21	Capture TCP traffic to or from port 21 (typically the FTP command channel)
portrange 1-80	Capture UDP/TCP traffic to or from ports from 1 through 80
tcp portrange 1-80	Capture TCP traffic to or from ports from 1 through 80
host 10.3.1.1 and port 80	Capture UDP/TCP traffic to or from port 80 that is being sent to or from 10.3.1.1
icmp[0]=8	Capture all ICMP Type 8 (Echo Request) packets.

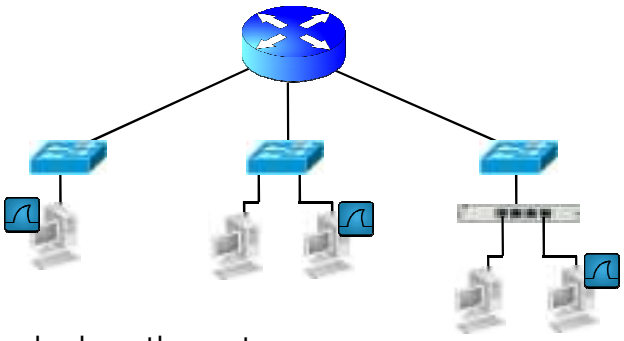
23

Capture – where ?



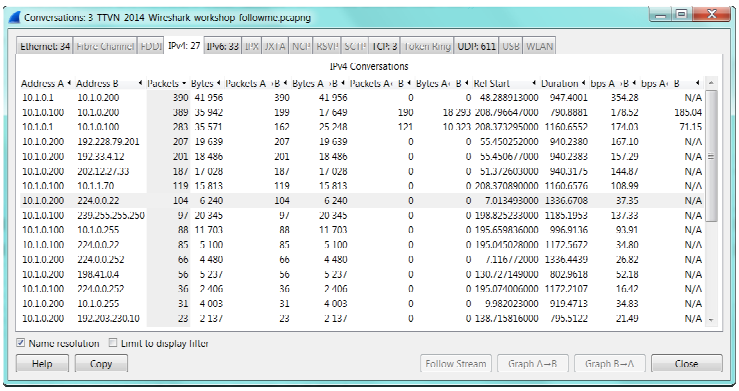
24

Capture options



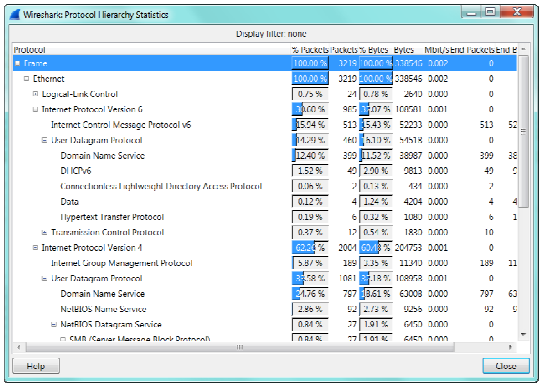
- Run Wireshark on the system
- Configure mirror or span port on Layer2/3 switch, run Wireshark on separate device
- Install a "Tap" between system and switch, run Wireshark on separate device

Top talkers



- Determine top talkers based on MAC addresses, IPv4/IPv6 addresses, port numbers, etc.
- Select: >Statistics >Conversations

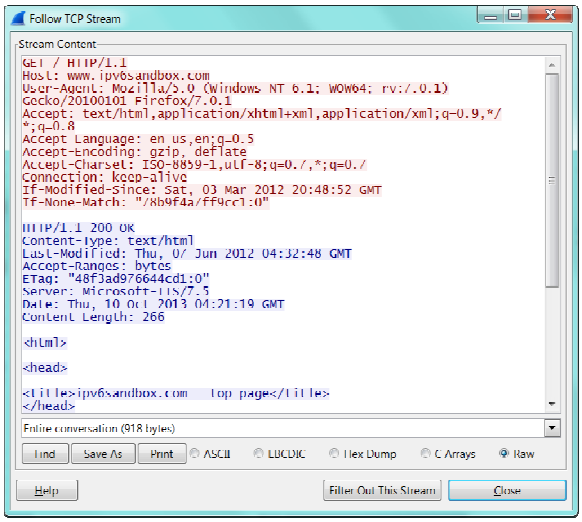
Identify applications & protocols



- Identify application and protocols running on the network
- Select: >Statistics >Protocol Hierarchy

27

Follow streams



- Follow Streams
  - TCP
  - UDP
  - SSL
- Select packet (if known 1st in sequence)
- >Analyze > Follow TCP Stream

28

Wireshark demo – follow me

- Sequence flow
  - watch me on this one
- Open "Wireshark-workshop-follow-jeff.pcapng"
  - Look for these protocols:
    - Telnet
    - SSH
    - HTTP
    - DNS

Wireshark lab #1

- Open "Wireshark-workshop_lab-file.pcapng"
- Create your own named profile
- Change time/date to time (only) and in milliseconds
- Create/save pkt_comment filter

Wireshark lab #2

- Find 1st pkt with dns.qry.name == "www.ipv6sandbox.com"
  - make a note as to which pkt this is
- Find 1st pkt with DNS query response for www.ipv6sandbox.com
  - make a note as to which pkt this is
  - what is the IP address in the answer section

Wireshark lab #3

- Find pkt with http.host == "www.ipv6sandbox.com"
  - make a note as to which pkt this is
- Find pkt with an http response code of 200
  - make a note as to which pkt this is
- Find pkt with comment of 'this is the secret pkt with the most important comment!'

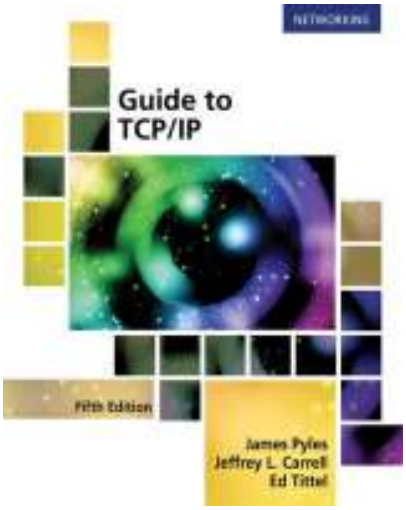
Wireshark 101

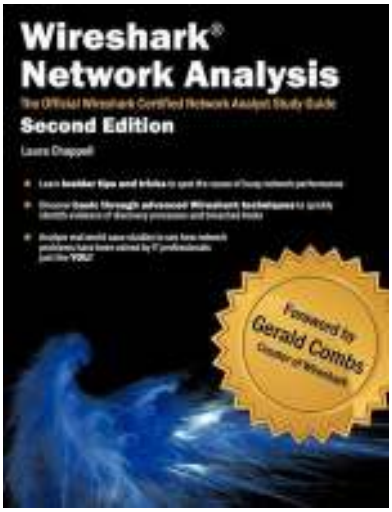
Questions ???

Resources

- https://wiki.wireshark.org/SampleCaptures
- https://www.netresec.com/?page=PcapFiles
- https://github.com/chrissanders/packets
- https://www.cellstream.com/resources/wireshark-profiles-repository

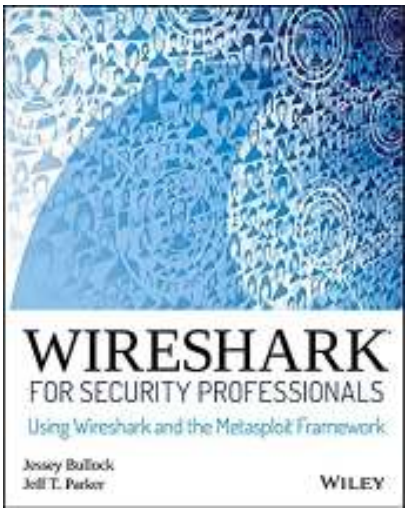
Resources

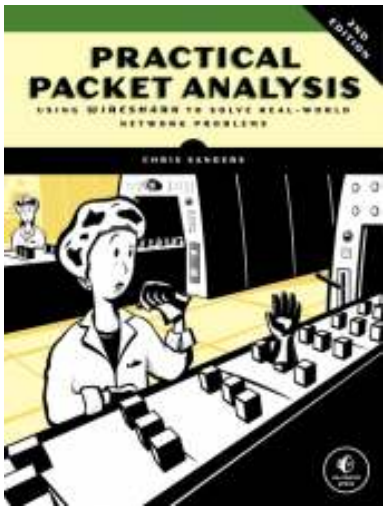




 35

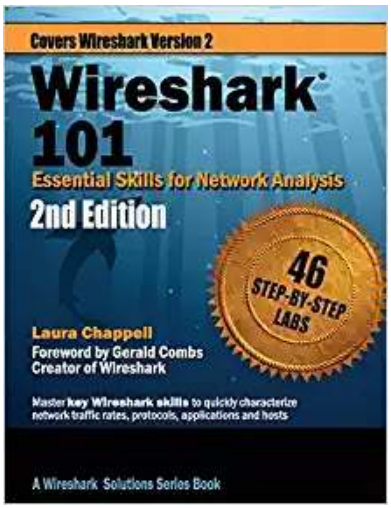
Resources

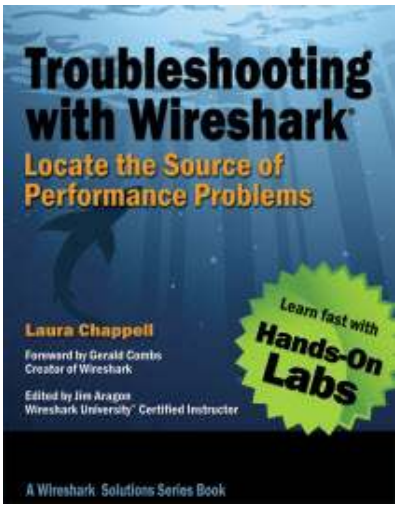




 36

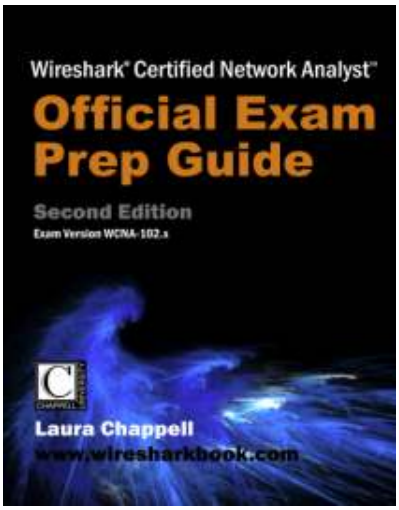
Resources





 37

Resources



 38

Thank You for Attending!

- Jeffrey L Carrell
- Network Instructor
- jeff.carrell@teachmeipv6.com

39